REMARKS/ARGUMENTS

I. Status of Claims

- Claims 1 and 16 are Independent Claims.
- Claims 1-10, 12-24 and 26-27 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Bommareddy et al (US Pat. No. 6,880,089) (hereinafter referred to as **Bommareddy**).
- Claims 11 and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over **Bommareddy** in view of Goseva-Popstojanova et al. (US Publ. No. 2003/0033542) (hereinafter referred to as **Goseva-Popstojanova**).

II. Response

A. Bommareddy's cleansing cycle involves different mechanisms when compared to the claimed invention's transfer and self-cleansing mechanisms.

The MPEP states that to anticipate a claim, the cited prior art reference must teach every element of the claim. See MPEP § 2131; see also Verdegaal Bros. v. Union Oil Co. of CA, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

1. Bommareddy monitors the operational health of firewalls, whereas the claimed invention does not teach such monitoring.

Bommareddy teaches a firewall clustering system that continually monitors the operational health of firewalls. See **Bommareddy**, col. 3, ll. 35-37 and col. 7, ll. 23-26. To achieve this goal, **Bommareddy** uses internal and external network flow controllers **810**. Id. at Fig. 8 and col. 8, ll. 20-22. Apparently as the key inventive entity of **Bommareddy's** invention,

the network flow controller is designed to enforce HTTP traffic redirection to proxy servers, as well as control redirection of other IP traffic. Id. at col. 20, ll. 58-65 and col. 21, ll. 10-15.

To ensure that the servers are operational, these network flow controllers implements server fault-intolerance within a cluster. See **Bommareddy**, col. 21, ll. 17-20. In testing whether the servers are operational, a network flow controller would ping, at regular intervals, each server with application probes and await a reply. Id. at col. 8, ll. 20-26 and col. 21, ll. 16-19. If a server fails to respond, then **Bommareddy** classifies such failed server as being "down." Id. at col. 21, ll. 21-24. If and when a server is down, then the network flow controllers would reroute any packets bound for the down server to the most suitable servers within the cluster. Id. at col. 21, ll. 25-31.

Additionally, **Bommareddy** applies this type of operational health monitoring to firewalls and routers. See **Bommareddy**, col. 8, ll. 20-26 and col. 21, l. 52 – col. 22, l. 40.

Here, the claimed invention (the self-cleansing intrusion tolerance system (SCIT)) does not monitor the operational health of any system component. Rather, it discloses a self-cleansing mechanism that automatically cleanses a subsystem (e.g., a firewall, server, gateway, etc.) on a cyclically timed-basis. See **Specification**, Figs. 1-5, paras. [0023]-[0024], [0038]. Serving as a key inventive entity, the self-cleansing mechanism renders operational health monitoring unnecessary.

Furthermore, the claimed invention makes no determination as to whether a subsystem has been compromised by an intrusion. Instead, the claimed invention assumes that a subsystem has failed. See **Specification**, para. [0022]. Thus, by making such decision, the subsystem enters into a cleaning cycle. Id.

Automatic cleansing occurs whether a fault in an active subsystem is detected, an intrusion into an active subsystem is detected, or a predetermined amount of time has lapsed since the last transfer cycle. See **Specification**, para. [0040]. As such, even if an intrusion was successful, the intrusion would be limited to a very short window of one fast, self-cleansing cycle. Id. at paras. [0043], [0044] and [0057].

Hence, because **Bommareddy's** operational health monitoring is not present in the claimed invention, **Bommareddy** cannot read upon the claimed invention. Therefore, Applicants respectfully request that Examiner withdraw these rejections.

2. Bommareddy actively detects firewall failures, whereas the claimed invention does not make such detection.

Bommareddy actively looks for firewall failures via its operational health monitoring feature (i.e., testing the operational state of the firewall with Ping packets). See **Bommareddy**, col. 8, ll. 20-26. According to **Bommareddy**, the firewall clustering system detects one or more various failure conditions. These include: "(1) failure of the firewall internal LAN interface and link , (2) failure of the firewall external LAN interface and link, and (3) failure of the firewall due to power outage, software malfunction, hardware malfunction, or other condition." Id. at col. 7, ll. 27-33.

Each of the network flow controllers maintains a list of operational firewalls. See **Bommareddy**, col. 4, ll. 59-60 and col. 9, ll. 5-7. So long as the firewall remains operational, it can be used by both internal and external network flow controllers for every inbound and outbound packet. Id. at col. 4, l. 66 – col. 5, l. 2 and col. 9, ll. 13-16. However, when a failure is detected, traffic is automatically diverted to the remaining operational firewalls in both inbound and outbound directions. Id. at col. 7, ll. 33-36.

In contrast, the self-cleansing intrusion tolerance system (SCIT) of the claimed invention does not actively detect failures in firewalls. As mentioned above, there is no need for intrusion detection because it assumes that the server has been compromised as soon as it is connected to an internal and/or external network (e.g., the Internet). See, e.g., **Specification**, paras. [0022], [0047] (assuming that a failure has occurred after being connected to an internal network). Using this assumption, SCIT causes each subsystem to automatically enter a cleansing cycle. Whether there has been a failure and/or a breach, either or both will be short-lived because of the cleansing cycle. Id. at para. [0044].

Hence, SCIT is not concerned with whether such failures occur. By relying on automatic cleansing cycles, SCIT does not have to actively seek out intrusions or failures. With this significant difference, Applicants believe **Bommareddy** does not read upon the claimed invention. Thus, withdrawal of these rejections is respectfully requested.

B. In consideration of Dependent Claims 11 and 25, the combination of Bommareddy and Goseva-Popstojanova teaches away from the claimed invention.

Goseva-Popstojanova teaches an intrusion communication network that places emphasis on the continuity of operation and an attack-survivable communication network. See **Goseva-Popstojanova**, Abstract. **Goseva-Popstojanova's** attack-survivable communication network operates in one of the following ways: (1) "entering a vulnerable state from the good state once the communication network becomes vulnerable to intrusion"; (2) "screening for vulnerability to intrusion which would cause the communication network to transition to a vulnerable state to eliminate at least one of the vulnerabilities detected while screening the communication network

so as to return the communication network to the good state"; or (3) detecting vulnerabilities by screening for vulnerability exploitations in the communication network. Id. at paras. [0009]-[0011].

In each of these three ways, an attack or pre-attack must be caused by a user before **Goseva-Popstojanova's** system enters into a vulnerability state. See **Goseva-Popstojanova**. para. [0024]. Alternatively, the strategies for resistance must fail. Id. at para. [0026]. When either case occurs, **Goseva-Popstojanova** teaches the implementation of four post-attack phases that form the basis of the system's all fault tolerance techniques. Id. at para [0028]. These phases are (a) error detection; (b) damage assessment; (c) error recovery; and (d) fault treatment and continued service. Id. Of relevance to this response are the first two. See Office Action, 6, part 5 (05/31/2007).

Examiner correctly states that **Goseva-Popstojanova** teaches the step of auditing in its system cleansing actions. See **Goseva-Popstojanova**, para. [0029] ("Strategies, for (a) error detection and (b) damage assessment include intrusion detection (i.e., anomaly based and signature based detection), logging, and auditing."). **Goseva-Popstojanova** explains that "auditing provides for an independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changed in controls, policy, or procedures." Id. However, this auditing stage occurs as part of a post-attack phase. In other words, after the system has been attacked, intruded, or detected an attack or intrusion, it would then detect errors and assess damages by detecting other intrusions, logging events and auditing the system.

Thus, when combined with **Bommareddy**, the combination of **Bommareddy** and **Goseva-Popstojanova** must first be working and then be attacked or detect an intrusion. Then,

and only then, would the combination be cleansed. The auditing activity would take effect after the attack or intrusion.

Unlike the combined prior art, Applicants' system auditing takes effect in various stages. For example, auditing may occur during SCIT's measurable events, cleansing cycle or system performance checks. See **Specification**, para. [0034]. The cleansing cycle may be described as one subsystem being activated or working (e.g., remain online), while another subsystem being deactivated (e.g., brought offline) and self-cleansed by rebooting and integrity checking. See **Specification**, para. [0043].

Moreover, another significant difference is that Applicants' claimed invention does not wait for an attack or an intrusion to occur first. As explained above, Applicants' claimed invention assumes that the system has been attacked or intruded and thus, automatically cleanses itself after a certain time period. See supra, part II.A.1 and II.A.2, **Specification**, para. [0022], [0044]. Simply, Applicants' claimed invention would cleanse itself whether or not an attack or intrusion has occurred. See supra, part II.A.1 and II.A.2.

Because of these differences, Applicants believe the combination of **Bommareddy** and **Goseva-Popstojanova** does not read upon Applicants' claimed invention. Therefore, Applicants respectfully request that these rejections be withdrawn.

C. Dependent Claims 2-15 and 17-27 depend on Independent Claims.

Because Dependent Claims 2-15 and 17-27 ultimately depend on their respective independent claims, the arguments presented for the independent claims also apply to these dependent claims. Therefore, Applicants respectfully request withdrawal of these objections.

Respectfully submitted,

/David Yee, Reg. No. 55,753/
David Yee
Registration No. 55,753

Office of Technology Transfer
George Mason University
4400 University Dr., MSN5G5
Fairfax, VA 22030
Phone/Fax: 703-993-3949

Filed: August 31, 2007